US007036019B1

(12) **United States Patent**
Saito

(10) **Patent No.: US 7,036,019 B1**
(45) **Date of Patent: Apr. 25, 2006**

(54) **METHOD FOR CONTROLLING DATABASE COPYRIGHTS**

(75) Inventor: **Makoto Saito**, Tokyo (JP)

(73) Assignee: **Intarsia Software LLC**, Las Vegas, NV (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/544,497**

(22) Filed: **Apr. 7, 2000**

Related U.S. Application Data

(63) Continuation of application No. 08/895,493, filed on Jul. 16, 1997, which is a continuation of application No. 08/416,037, filed on Mar. 31, 1995, now abandoned.

(30) **Foreign Application Priority Data**

Apr. 1, 1994 (JP) 6-64889

(51) **Int. Cl.**
H04K 1/00 (2006.01)
H04L 9/00 (2006.01)

(52) **U.S. Cl.** **713/193**; 713/200; 705/57; 705/59

(58) **Field of Classification Search** 713/180, 713/155, 202, 193; 380/29, 33, 43, 45, 46, 380/47, 51, 57, 239, 259, 262, 277, 280, 380/281; 705/62, 57, 59
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,386,233	A	*	5/1983	Smid et al.	380/281
4,588,991	A		5/1986	Atalla	
4,827,508	A		5/1989	Shear	
5,138,659	A		8/1992	Kelkar et al.	
5,224,163	A		6/1993	Gasser et al.	380/30
5,235,641	A		8/1993	Nozawa et al.	
5,301,245	A		4/1994	Endoh	
5,345,508	A	*	9/1994	Lynn et al.	380/46
5,353,351	A	*	10/1994	Bartoli et al.	380/33

(Continued)

FOREIGN PATENT DOCUMENTS

EP	0 398 645	11/1990
EP	0 581 227	2/1994
EP	0 590 763	4/1994
EP	0 649 074	4/1995

OTHER PUBLICATIONS

Gale, B. and Baylin, F., Scrambling and Descrambling, Satellite and Cable TV 2nd Ed, Baylin/Gale Productions 1986 Boulder CO; pp. 163–165.

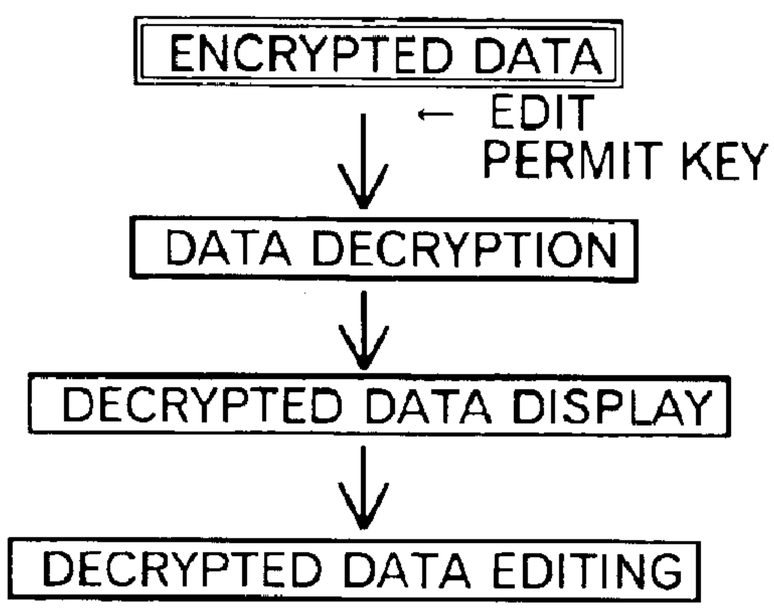
Research Disclosure No. 335, Mar. 1992, EMSWORTH GB, p. 219 XP 000301128 "Encryption of Information to be Recorded so as to Prevent Unauthorized Playback."

Primary Examiner—Hosuk Song
(74) *Attorney, Agent, or Firm*—Berkeley Law & Technology Group

(57) **ABSTRACT**

The present invention provides a method for controlling copyrights of digital data in a database system including real time transmission of a digital picture. Copyrights are controlled using one or more of the following, as necessary, in addition to a permit key: a copyright control program, copyright information or copyright control message. The copyright control program, the copyright information and the copyright control message are supplied together with the permit key, or they are supplied together with the data. Otherwise, a part of them is supplied together with the permit key and the other part of them is supplied together with the data. The data, the permit key, the copyright control message, the copyright information and the copyright control program are (1) transmitted while encrypted, but are decrypted when used, or (2) they are transmitted while encrypted and decrypted for display only, otherwise remaining encrypted, or (3) they may not be encrypted at all.

28 Claims, 4 Drawing Sheets



U.S. PATENT DOCUMENTS

5,381,480	A	*	1/1995	Butter et al.	380/37
5,392,351	A	*	2/1995	Hasebe et al.	705/51
5,400,403	A		3/1995	Fahn et al.	380/21
5,457,746	A		10/1995	Dolphin	380/4
5,465,299	A		11/1995	Matsumoto et al.	380/23
5,485,577	A	*	1/1996	Eyer et al.	713/202
5,495,533	A		2/1996	Linehan et al.	380/21
5,504,816	A		4/1996	Hamilton et al.	
5,504,818	A		4/1996	Okano	395/49
5,606,613	A	*	2/1997	Lee et al.	705/62
5,646,999	A		7/1997	Saito	380/25
6,069,952	A	*	5/2000	Saito et al.	705/57

* cited by examiner

FIG. 1A

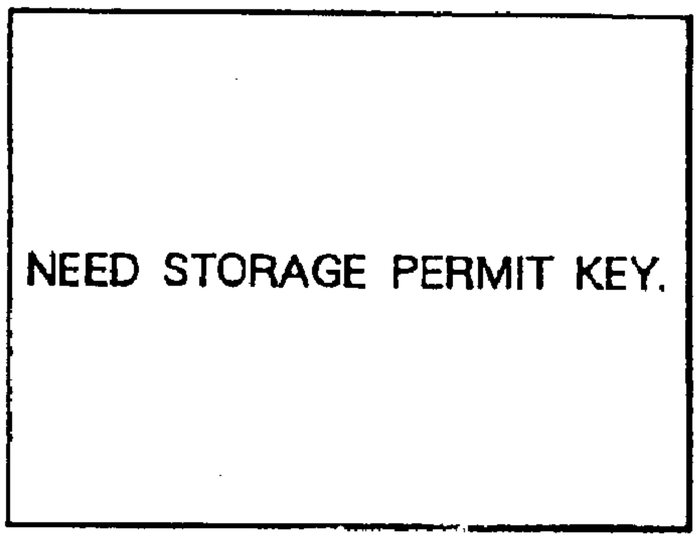


FIG. 1B

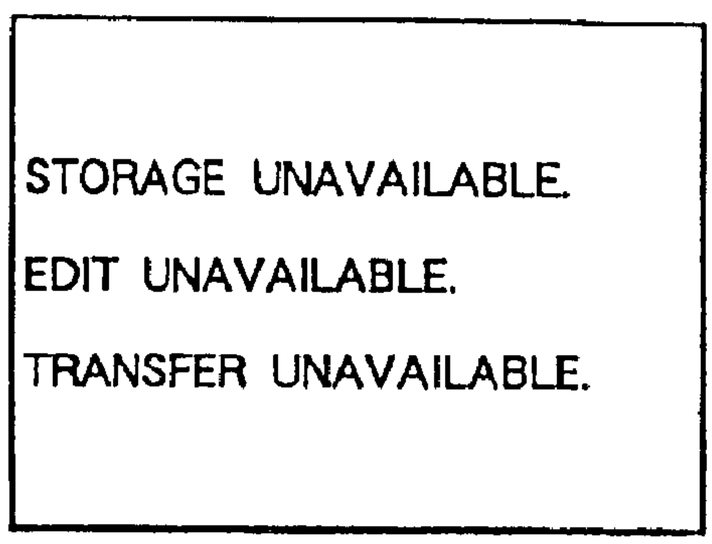


FIG. 2A

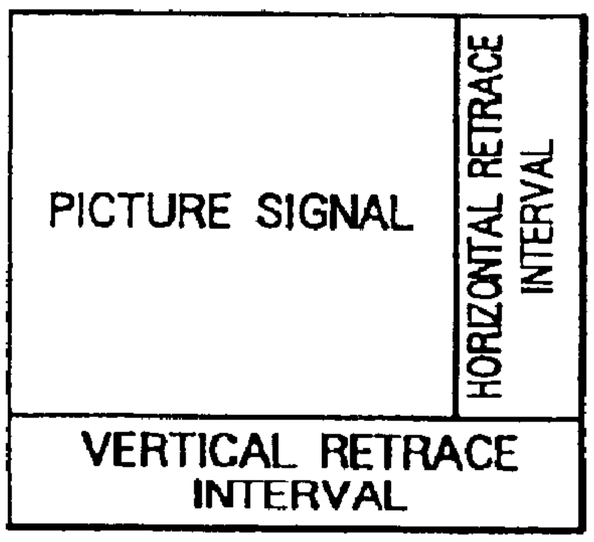


FIG. 2B

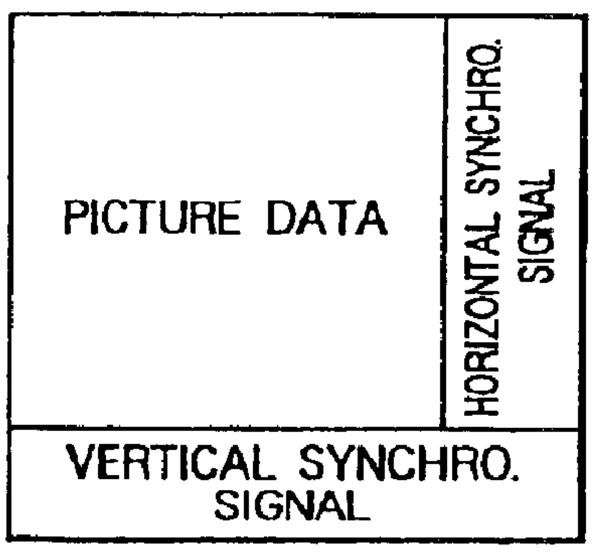


FIG. 3A

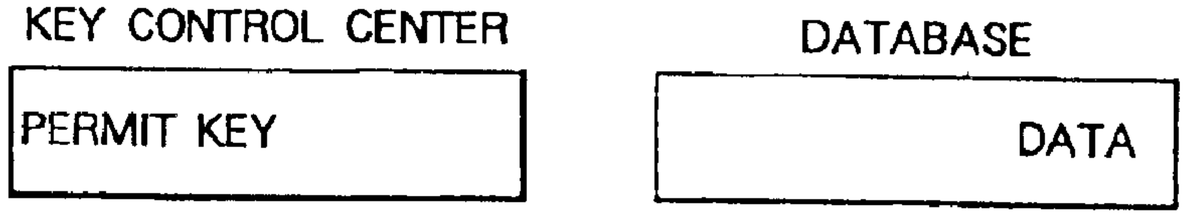


FIG. 3B

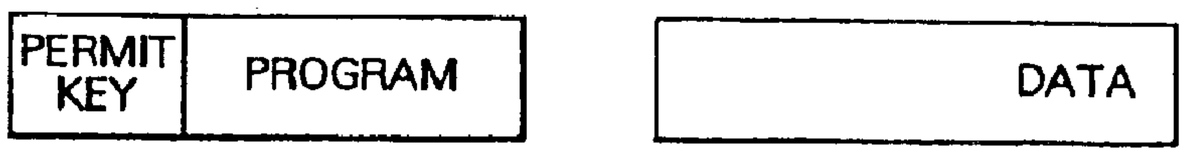


FIG. 3C

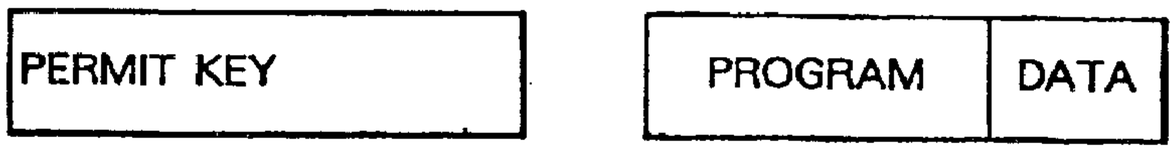


FIG. 3D

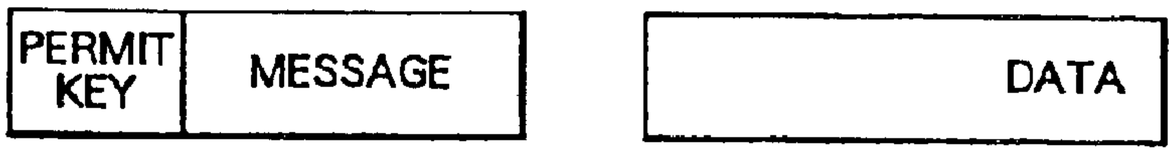


FIG. 3E

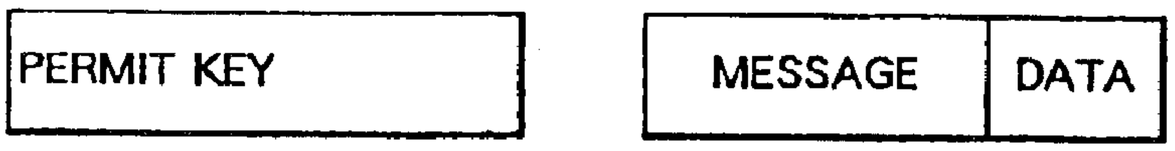


FIG. 3F

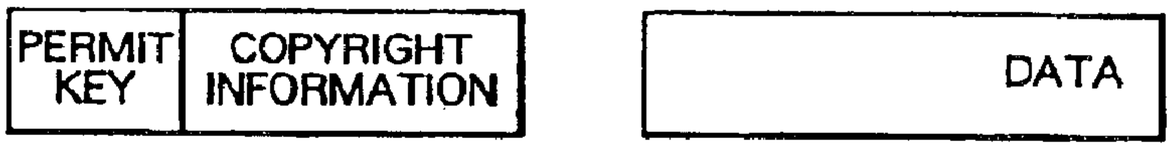


FIG. 3G

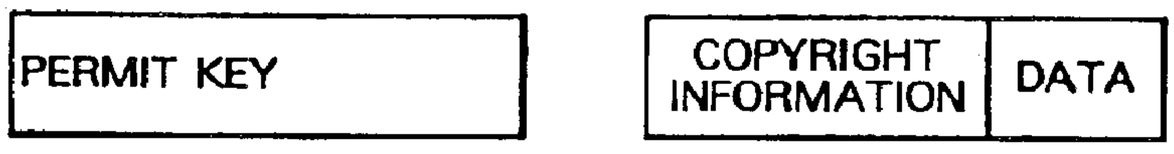


FIG. 3H

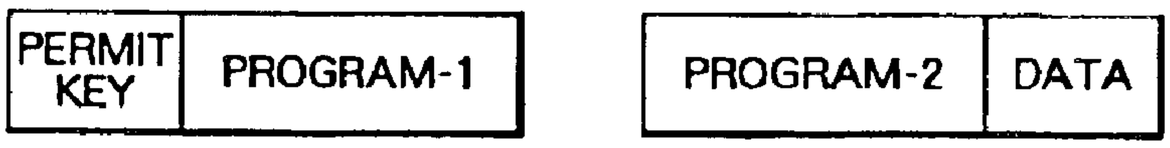


FIG. 3I

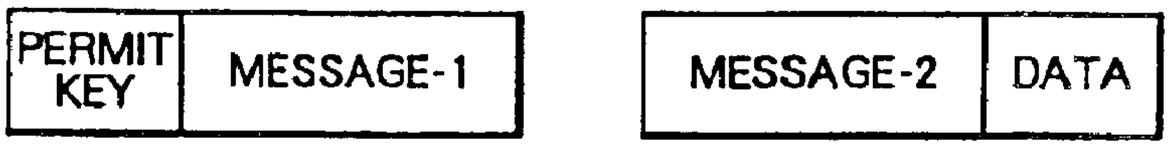


FIG. 3J

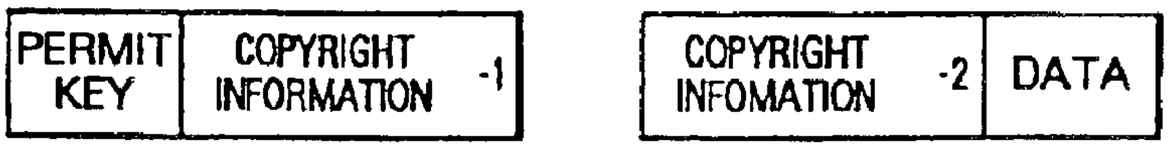


Fig.4A

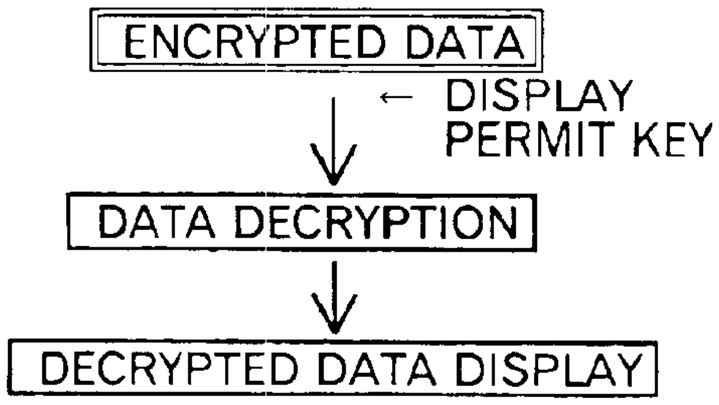


Fig.4B

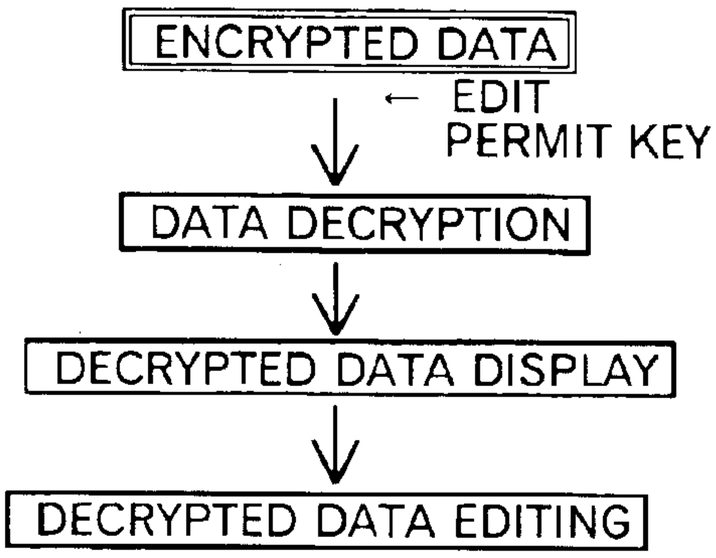


Fig.4C

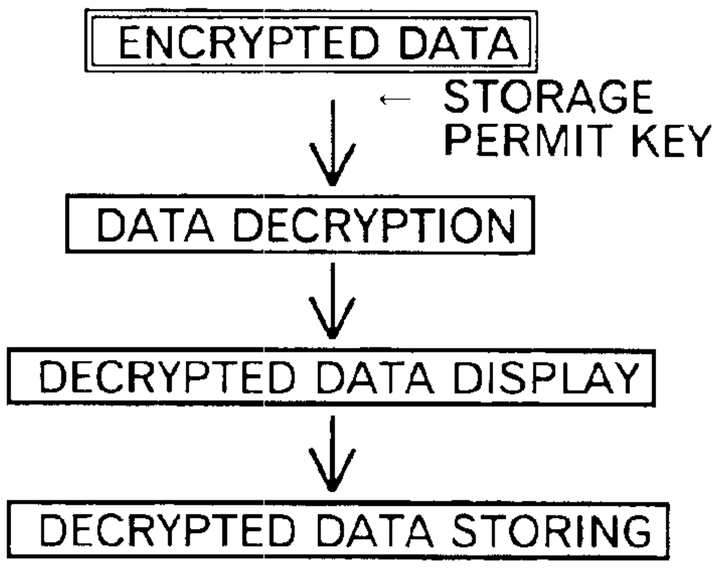


Fig.4D

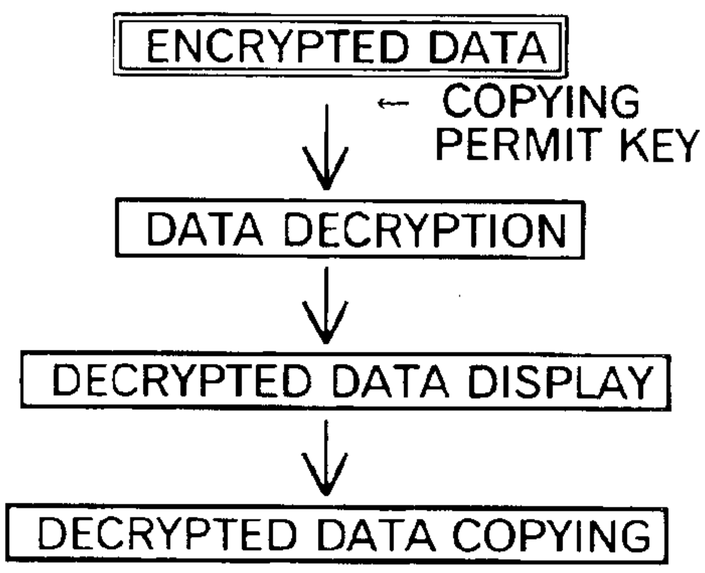


Fig.4E

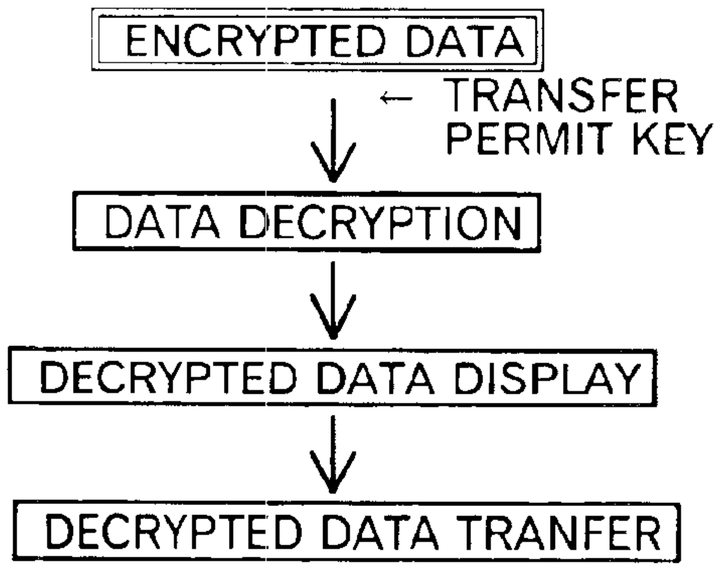


Fig.5A

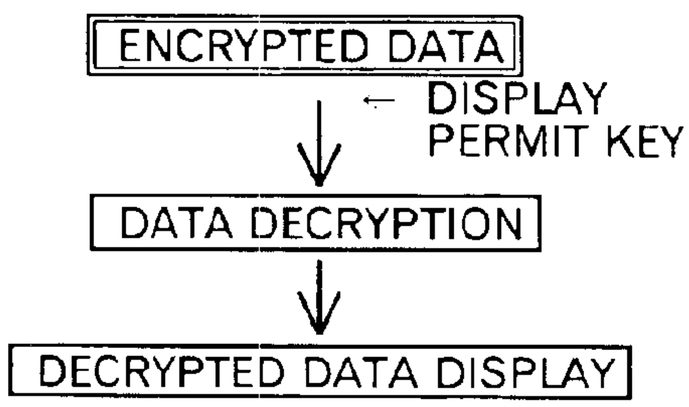


Fig.5B

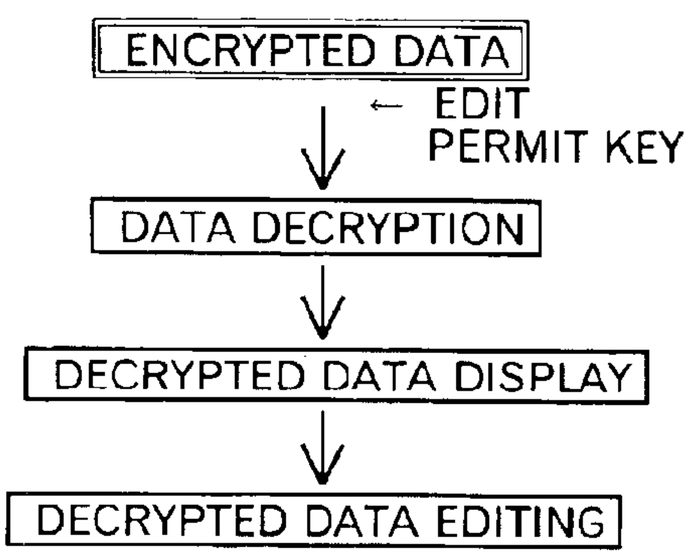


Fig.5C

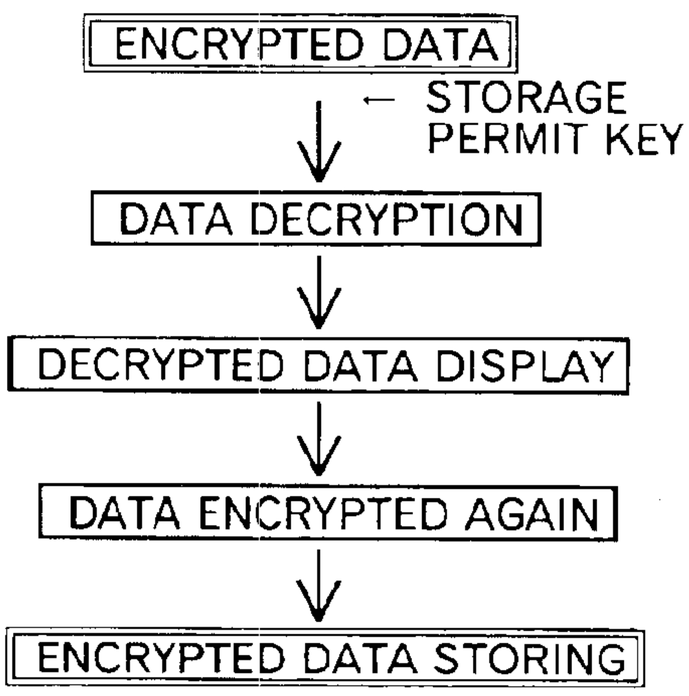


Fig.5D

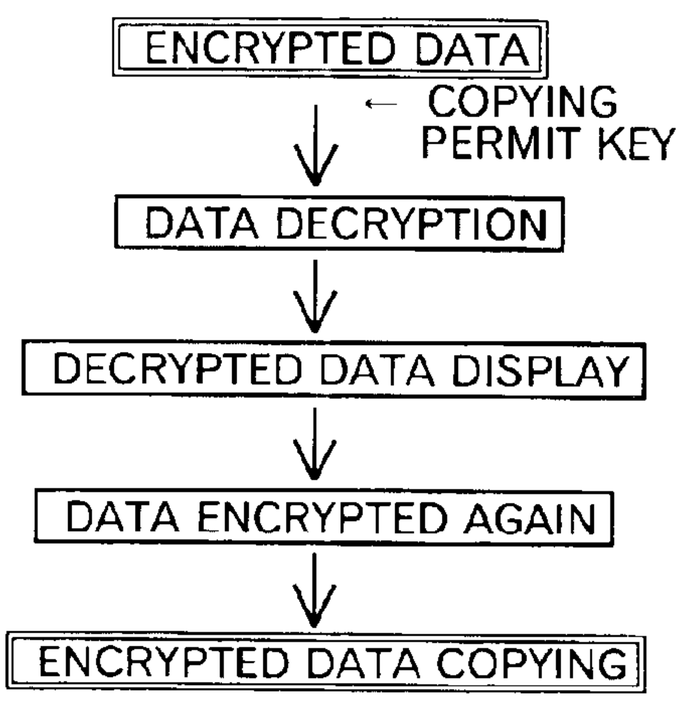
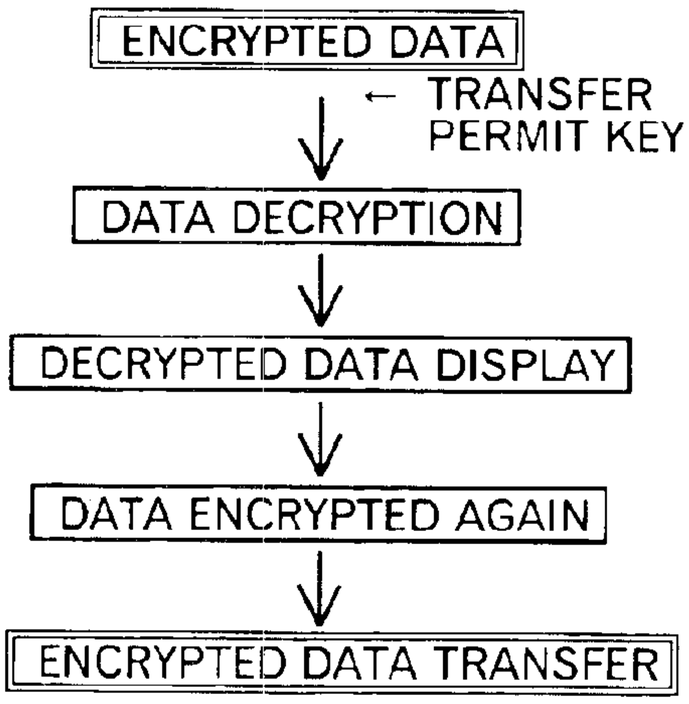


Fig.5E



METHOD FOR CONTROLLING DATABASE COPYRIGHTS

This application is a Continuation of prior application Ser. No. 08/895,493 filed Jul. 16, 1997, which is a Continuation of prior application Ser. No. 08/416,037 filed Mar. 31, 1995, which has been abandoned.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to a method for controlling copyrights or utilizing, storing, copying, editing and transferring of digital data, and in particular, to an application of the method to a multimedia system.

2. Background Art

In the information oriented society of today, database systems are becoming wide spread in which it is possible to use various types of data, stored independently by each computer in the past, by connecting computers via communication lines.

In such a database system, the information handled up to this point has been conventionally coded information that can be processed by computer, and that contains a relatively small amount of information and monochrome binary data, such as facsimile information at the most. It is not possible to handle data containing a relatively large amount of information, such as data for natural pictures or animation.

With the rapid progress of digital processing techniques for various types of electrical signals, a technique is under development for digital processing of picture signals other than binary data, handled only as analog signals in the past.

By digitizing the picture signal, it is possible to handle a picture signal, such as television signal, by computer. As a technique of the future, attention is now focused on "multimedia systems", which can simultaneously handle the data processed by computers and digitized picture data. Because the picture data contains an overwhelmingly large amount of information compared with character data and audio data, it is difficult to store, transfer or process the picture data by computer. For this reason, techniques for compressing and expanding picture data have been developed. Further, several standards for compression/expansion of picture data have been established. For example, the following standards have been established as common standards: JPEG (Joint Photographic image coding Experts Group) standards for still pictures, H.261 standards for television conferences, MPEG1 (Moving Picture image coding Experts Group 1) standards for picture accumulation, and MPEG2 standards to cope with current television broadcasting and high definition television broadcasting. By implementing these new techniques, it is now possible to transmit digital picture data in real time.

For analog data, which has been widely used in the past, the control of copyrights during processing has not been an important issue because the quality of the analog data deteriorates each time the data is stored, copied, edited or transferred. However, the quality of digital data does not deteriorate even when the data is repeatedly stored, copied, edited or transferred. Therefore, the management and control of copyrights during processing of digital data is an important issue.

Up to now, there has been no adequate method for management and control of copyrights for digital data. It has been managed and controlled merely by copyright law or by contracts. In copyright law, only compensation for digital sound and picture recording devices has been prescribed.

It is possible not only to refer to the content of a database, but also to effectively utilize the data obtained from the database by storing, copying or editing the data, and also transferring the edited data to other persons or to the database with the edited data registered as new data.

In a conventional database system, only character data is handled. However, in multimedia systems, sound data and picture data, which are originally analog data, are digitized and used as part of the database in addition to the other data in the database, such as character data.

Under such circumstances, it is an important question as to how to handle copyrights of the data in the database. However, there are no means in the prior art for copyright management and control of such actions as copying, editing, transferring, etc., of data.

A system for executing copyright control by using encrypted data and obtaining a permit key from a key control center via public telephone lines is disclosed in Japanese Patent Application 4-199942 (US-08/098415) and Japanese Patent Application 4-289074 (US-08/143912) of the present inventors. A device for this purpose is disclosed in Japanese Patent Application 4-276941 (US-08/135634), also of the present inventors.

SUMMARY OF THE INVENTION

It is an object of the present invention to provide a method for controlling copyrights in the display (including the process of providing sound), storage, copying, editing and transfer of digital data in a database system including real time transmission of digital pictures.

For the control of copyrights in the database system to which the present invention is applied, it is essential to transmit one or more of copyright information; ie., messages of copyright control, information about copyrights and a program for controlling copyrights, when necessary, in addition to a key for enabling users who wish to use encrypted data.

The copyright control message is displayed on a screen and advises or warns the user if the data is being utilized in a manner inconsistent with the conditions of the user's request or permission. The copyright control program watches and controls data use so that the data is not utilized beyond the conditions of the user's request or permission.

The copyright control program, the copyright information and the copyright control message are supplied together with a permit key in some cases, but they may also be supplied together with data in other cases. It is also possible to supply a part of them together with the permit key, and to supply the other part with the data.

For the data, the permit key, the copyright control message, the copyright information and the copyright control program, there are the following three cases: they are transmitted in encrypted form and decrypted upon use; they are transmitted in encrypted form and decrypted only when they are displayed; or they are not encrypted at all.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1**A and FIG. **1**B illustrate examples of display messages of the present invention.

FIG. **2**A and FIG. **2**B illustrate structures for television signals.

FIG. **3**A to FIG. **3**J illustrate embodiments of the present invention.

FIGS. **4**A–**4**E illustrate structures of embodiments of the present invention.

FIGS. **5**A–**5**E illustrate structures of embodiments of the present invention.

DETAILED DESCRIPTION

In the following, description will be given on embodiments of the present invention.

In the prior patent applications mentioned above, it is assumed that a permit key obtaining route is different from a data obtaining route as shown in FIG. **3**A, and that the permit key is obtained from a key control center via public telephone lines. However, if a charging method is determined, it is possible to obtain the permit key via the communication system through which the database is supplied.

In the system of the prior patent applications, it is assumed that the permit key for secondary exploitation is used for distribution of the data selected from secondary exploitation. Secondary exploitation involving the storing, copying, editing, transferring, etc. of data is not included in the assumption. Also, it is assumed that the data is distributed only inside a LAN to which the users belong. Distribution outside the LAN is not part of the assumption. Therefore, the system is not adequate to cope with secondary exploitation unless the users choose to honor the copyright.

To cope with various forms of the secondary exploitation as described above, a plurality of permit keys are prepared to match each form of use, and no utilization is possible unless there is a permit key suitable for the desired form of use. As to the forms of use available for a database, there are display, storage, copying, edit, transfer, etc. Examples of these utilization forms as shown in FIGS. **4**A to **4**E. FIG. **4**A illustrates a case when supplied encrypted data is displayed. The encrypted data is decrypted by a display permit key, and the data thus decrypted is displayed. FIG. **4**B illustrates a case when supplied encrypted data is edited. The encrypted data is decrypted by an edit permit key, and the data thus decrypted is displayed, and then editing is performed. FIG. **4**C illustrates a case when supplied encrypted data is stored. The encrypted data is decrypted by a storage permit key, and the data thus decrypted is displayed, and then storing is performed. FIG. **4**D illustrates a case when supplied encrypted data is copied. The encrypted data is decrypted by a copy permit key, and the data thus decrypted is displayed, and then copying is performed. FIG. **4**E illustrates a case when supplied encrypted data is transferred. The encrypted data is decrypted by a transfer permit key, and the data thus decrypted is displayed, and then transfer is performed. In these Figures, double-framed parts show that data is encrypted. The permit keys suitable for these forms of use should be prepared. However, in the case where the ability to execute several forms of use at the same time is desired, it is necessary to obtain a plurality of permit keys. If the user fails to obtain the permit keys, the desired form of use may not be executed.

To avoid such situations, a permit key can be used which makes it possible to execute several forms of use. Hierarchical permit keys can be used such that an upper level key also fulfills the function of a lower level key. For example, from lower level to upper level, the hierarchy is defined as: display<storage<copying<edit<transfer. With the display permit key, only display operations can be executed. Display and storage operations can be executed by the storage permit key. Display, storage and copying operations can be executed by the copying permit key. Display, storage, copying and edit operations can be executed by the edit permit key. Display, storage, copying, edit and transfer operations can be executed by the transfer permit key.

In the prior patent application, i.e. Japanese Patent Application 4-276941 (US-08/135634), the present inventors have proposed a system in which a plurality of encrypted data, each encrypted by one of a plurality of different crypt keys, are recorded (stored) in encrypted form. The data is decrypted when it is utilized in the system where the storage permit key is the lowest level key.

By applying this system, it is possible to order key hierarchy from lower-level to upper-level in the order of: storage<copying<transfer<display<edit. Specifically, the order is set in such manner that storage operations can be executed by a storage permit key; storage and copying operations can be executed by a copying permit key; storage, copying and transfer operations can be executed by a transfer permit key; storage, copying, transfer and display operations can be executed by a display permit key; and storage, copying, transfer, display and edit operations can be executed by an edit permit key.

In this system, storage, copying and transfer are placed at a lower level than display because, even when storage, copying and transfer operations are executed on the data, it is difficult and meaningless to utilize the data since it cannot be displayed. It is necessary to execute display in order to utilize the data. This hierarchical arrangement is best suited to a system, in which encrypted data are supplied and are utilized using a permit key.

The permit key is usually offered to the user on payment basis. Therefore, except where data utilization is unlimited, the number of times the permit key may be used is limited to one time or several times if it is necessary to limit the number of times the data is used.

Because the data can be used if there is a permit key, it is possible to use the data beyond the permitted range if the permit key is duplicated or falsified. To prevent this, the permit key is encrypted.

The use of data includes storage, display, copying, edit, transfer, etc. thereof, which are necessary to be allowed or prohibited.

In the case where it is necessary to limit the number of usage times or to limit forms of use, it is desirable to display a message for such purpose.

In the case where the information under copyright is falsified, the data supplier or the user may suffer damages. This must be prevented.

To ensure complete copyright control, information on the original copyright and information on secondary and tertiary copyrights for the edition of the data are given to the data.

The above copyright control is executed by the copyright control program.

In a conventional database system, the data itself is offered in a completely defenseless state. Therefore, copyright control can be executed only when data is taken out of the database. In the subsequent copyright control, there is no other way but to rely on conscience of the user and to take necessary measures when the data is utilized beyond the permitted range of use.

For this reason, as described in the prior patent application, i.e. Japanese Patent Application 4-276941 (US-08/135634), the data supplied from the database are left in an encrypted state, and storage is executed under this condition. In addition, copying and transfer are also executed in the encrypted state. Decrypting is performed only in display and edit operations, and these are controlled by the copyright control program. These examples are shown in FIGS. **5**A to **5**E.

FIG. 5A illustrates a case when supplied encrypted data is displayed. The encrypted data is decrypted by a display permit key, and the data thus decrypted is displayed. FIG. 5B illustrates a case when supplied encrypted data is edited. The encrypted data is decrypted by an edit permit key, and the data thus decrypted is displayed, and then editing is performed. FIG. 5C illustrates a case when supplied encrypted data is stored. The encrypted data is decrypted by a storage permit key, and the data thus decrypted is displayed, and then, the decrypted data is encrypted again by the storing permit key, and then storing is performed. Thus, the data encrypted again is stored. FIG. 5D illustrates a case when supplied encrypted data is copied. The encrypted data is decrypted by a copy permit key, and the data thus decrypted is displayed and then, the decrypted data is encrypted again by the copy permit key, and then copying is performed. Thus, the data encrypted again is copied. FIG. 5E illustrates a case when supplied encrypted data is transferred. The encrypted data is decrypted by a transfer permit key, and the data thus decrypted is displayed and then, the decrypted data is encrypted again by the transfer permit key, and then transfer is performed. Thus, the data encrypted again is transferred. In these Figures, double-framed parts show that data is with encrypted. In so doing, it is impossible to use the data beyond the permitted range. In this case, the copyright control program may be integrated with the data or may be encrypted.

Because the copyright control program is encrypted and the permit key decrypts the copyright control program, and because the copyright control program decrypts and encrypts the data, the data is encrypted twice.

In this case, if a crypt key unique to the data is added to the copyright control program for the purpose of encrypting the data, it is impossible to decrypt the data if the copyright control program is separated from the data.

In this copyright control program, even if the data is stored, copied or transferred within the permitted range of use, and if these operations are executed after the data and the copyright control program have been encrypted, it is impossible to use the data in an undesired manner.

If an operator uses a computer program inadequately and, as a result, the computer does not respond any more or computer operation is stopped, an error message is displayed so that the operator may know the cause. Similarly, if a user of the database erroneously uses the data beyond the permitted range of the permit key, and, as a result, the computer does not respond or operation is stopped, the user cannot understand the cause. In this case, a copyright control message is displayed just as an error message is displayed by the copyright control program.

The display of the copyright control message as described above also fulfills the function of providing a warning if the user intentionally uses the data beyond the range of use permitted by the permit key.

In general, various programs are incorporated into read-only memory (ROM) inside the equipment which the user uses, or the programs are supplied from software. When the programs are incorporated into ROM, there is no possibility that the programs may be changed. However, the equipment to be used is limited to systems that contain the ROM. On the other hand, when the programs are supplied from software, there is no system limitation if the programs are transferred. However, there is a possibility that the programs may be altered.

The database is utilized by various users using various types of devices. Therefore, if the programs for controlling copyrights are supplied as software, it is necessary to cope with various types of devices. Further, alteration of the programs must not be possible. Therefore, the copyright control program should be encrypted to prevent such trouble. In this case, it is necessary to modify the program according to the device that the user uses. A program to translate the copyright control program is provided in the communication software of the device which the user uses. The copyright control program can then be translated by the translation program so that it suits the device.

Even though the permit key for using the database may become more complicated due to encryption, a data size of several tens of bites is sufficient. Therefore, the time required for transmitting the permit key is far shorter than one second. In other words, even when a payment-based public telephone line is used and other information is transmitted together with the permit key, the increase of cost is negligible.

Therefore, when transmitting the permit key as shown in FIG. 3B, utilizing surplus time, the copyright control program can be transmitted.

The copyright control program can be supplied together with the permit key and also together with the data as shown in FIG. 3C.

In this case, the copyright control program is supplied together with the data, and the entire data utilization process is placed under control of the copyright control program. For example, the data supplied in encrypted form cannot be decrypted unless the copyright program supplied with it is used. If there is no such copyright control program, the data cannot be used. Thus, the control of copyrights is reinforced. Also, integration of the copyright control program with the data further reinforces copyright control.

The following are some examples of the copyright control message:

"Need a display permit key."

"Need a storage permit key."

"Need a copying permit key."

"Need a edit permit key."

"Need a transfer permit key."

Some other examples are:

"Display unavailable."

"Storage unavailable."

"Copy unavailable."

"Edit unavailable."

"Transfer unavailable."

These copyright control messages are displayed alone as shown in FIG. 1A or in combination as shown in FIG. 1B.

Next, descriptions will be given on supply of the copyright control message.

To display the copyright control message, the message must be stored in the memory of the device which the user uses. The memory in the device is classified as ROM and random-access memory (RAM).

The method of storing the messages in ROM is reliable, but there is a limitation to the device because the user must use the ROM wherein the copyright control messages are stored.

As for methods for storing messages in RAM, there is a method for supplying messages together with the permit key, a method for supplying messages together with the copyright control program, and a method for supplying messages together with the data. When the permit key and the copyright control program are supplied at the same time, the copyright control message can also be supplied at the same time.

The copyright control message is not effective unless an adequate message is displayed. For this reason, the copyright control message cannot play its designed role if the message is changed in such a manner that no substantial content is displayed, or further, if its content is deleted such that nothing is displayed. To prevent this trouble, the message is encrypted.

The display of the copyright control message is executed by the copyright control program. The modes of display are as follows. (1) When an operation is attempted with no adequate key available, a corresponding message is displayed. (2) All messages corresponding to operations available for the current permit key are displayed, if an operation is attempted without an available permit key.

The copyright control message is supplied together with the permit key as shown in FIG. **3**D, or together with the data as shown in FIG. **3**E.

The copyright control message is transmitted by transmitting all messages or only the necessary messages required. In the former case, the quantity of information is relatively large, but security is high. In the latter case, the quantity of information is relatively small, but security is low.

It is desirable that the copyright control message be inseparable from the data, as in the case of the copyright control program. This may be facilitated by integrating the copyright control message with the copyright control program.

To display the copyright on printed matter, the name of the author and the date are used. The copyright of the database is displayed by entering information such as the name of the author and the date.

As described above, edit and up-load of edited data are included in the use of the data in the database. Specifically, the presence of secondary data, which is edited from the data, i.e. a work of authorship, is recognized. To ensure the copyright of the data in this context, it is necessary to store the information on original authorship and secondary authorship together with the data. In case the data is used in a manner other than for down-loading and display, copyright information including information on the operator, in addition to the copyright information stored up to that moment, is stored together with the data as history.

In this case, only the person who controls the database can put the original authorship into the database as primary data. All data handled by other than the person in charge of database control is considered secondary data. Control of the data history is therefore further reinforced.

When the copyright information is separated from data which is a work of authorship, it becomes extremely difficult to recognize the copyright. Thus, it is necessary that the copyright information be inseparable from the data.

To prevent separation of the copyright information from the data, a method for integrating the data with the copyright information or a method for making the data unusable without copyright information are described. These methods are similar to the methods described above for the copyright control program and the copyright control message.

First, description will be given for a method for integrating the data with the copyright information.

The data handled by computer comprises a file header indicating data name and size, and a file body, which comprises the main body of data. Therefore, for integrating the data with the copyright information, there are methods that integrate the copyright information with the file header, that integrate the copyright information with the file body, and that take other means for the purpose.

Among these methods, the method that integrates the copyright information with file header, if the data is character information expressed with character code, is available even without a file header. Thus, the method is simple, but not very reliable. Also, because the capacity of the file header is not high, it is not sufficient if there is a large amount of copyright information.

Digital picture data and digital sound data are grouped together under a common group header. The copyright information can be integrated into this group header. However, there is a problem of header capacity similar to the case for the file header.

For the method of integrating the copyright information with the file body, one way is to add copyright information for each piece of data edited. Another way is to add the copyright information all together.

To add the copyright information for each edited piece of data, the copyright information is added to each piece of data which is edited by cut-and-paste procedure and produced. This is not only complicated but disadvantageous in that the entire file data becomes too big.

If the picture data indicates the copyright of original authorship, it is easy to identify corresponding data. Thus, it is not always necessary to add the copyright information to each minimum unit of the edited data.

It is also possible to write the copyright information into the copyright control program. In this method, it is difficult to manipulate the copyright information if it is written into the copyright control program integrated with the data as already described.

If the data is a picture signal, it is necessary to have synchronization signal data in order to define scanning line, field and frame. This synchronization signal has high redundancy and is generally represented with variable-length code. Thus, the copyright information can be mixed with the variable-length code. The number of scanning lines is 480 for VGA standards. By utilizing this method, a considerable quantity of information can be mixed into it.

In case the picture data is an animated picture, it is possible to write a sufficient quantity of copyright information in this method. However, if the picture data is a still picture edited by a cut-and-paste procedure, there may not be enough space to add the copyright information.

FIG. **2**A and FIG. **2**B represent structures for an analog television signal and a digital television signal. FIG. **2**A represents an analog television signal, and FIG. **2**B shows a digital television signal.

A signal containing other than picture data, such as the multiplex teletext signal in analog television, is inserted by utilizing the vertical retrace interval. The horizontal retrace interval is not utilized.

In contrast, in digital television, it is possible for a copyright control program or other multiplex teletext signal to be placed into horizontal scanning data or into vertical scanning data.

As a method for integrating the copyright information with data, one way is to write the copyright information into the data itself, and another is to write it into control code.

With the data used in computer, there is control code for controlling the communication system or computer system in addition to the data to be displayed on screen or used for some operation. This control code cannot be seen by the user. Therefore, if the copyright information is written into the control code, the copyright information thus written does not cause trouble for the user.

It is also possible to enter the copyright information into the files of the computer using the technique of a computer virus without affecting the operation itself.

The copyright information may be supplied together with the permit key as shown in FIG. **3**F of may be supplied together with data as shown in FIG. **3**G.

Attention has been focused in recent years on digital signatures. Using a private key, which only the person concerned knows, and a public key, which other persons also know, a digital signature is prepared from the private key and from the data on the file size of the document data. If the document data is changed, the change can be confirmed by the private key, and the content of the document data can be seen at any time by other persons using the public key. Thus, this scheme offers very high security.

The data in a computer can be changed without leaving any trace. Because of this, an author may not notice that his copyright is infringed, or a user may use the data without known that the content of the data has been changed, and the author or user may suffer damages. To prevent this, a digital signature is attached to the data, and damage to the copyright owner or the user can be avoided.

The permit key, copyright control program, copyright control message, and copyright information can be combined in any way as necessary to actualize the method for controlling database copyrights.

Also, it is possible to design in such a manner that only a part of the data of the copyright control program, the copyright control message or the copyright information is supplied together with the permit key as shown in FIG. **3**H, **3**I and **3**J, and that the other part is supplied together with the data to be utilized. The part supplied with the permit key and the part supplied together with the data are then combined, and the functions of the complete permit key maybe served after they have been combined together.

Thus, it is possible to give the function of the permit key to the copyright program and copyright control message, and higher security is ensured.

I claim:

1. A digital data management method, comprising the steps of:

encrypting digital data to produce encrypted digital data supplied to a user, using a utilization permit key predefined to permit at least one of displaying, editing, storing, copying, and transferring of said digital data;

decrypting said encrypted digital data to decrypted digital data by using a display permit key, which is utilization permit key permitting displaying of said digital data, and displaying said decrypted digital data;

decrypting said encrypted digital data to decrypted digital data by using a display permit key, which is said utilization permit key permitting displaying of said digital data, and displaying said decrypted digital data;

decrypting said encrypted digital data to decrypted digital data by using an edit permit key, which is said utilization permit key permitting editing of said digital data, and editing said decrypted digital data;

decrypting said encrypted digital data to decrypted digital data by using a storage permit key, which is said utilization permit key permitting storing of said digital data, encrypting again said decrypted digital data to encrypted digital data by using said storage permit key, and storing said encrypted digital data;

decrypting said encrypted digital data to decrypted digital data by using a copy permit key, which is said utilization permit key permitting copying of said digital data, encrypting again said decrypted digital data to encrypted digital data by using said copy permit key, and copying said encrypted digital data; and

decrypting said encrypted digital data to decrypted digital data by using a transfer permit key, which is said utilization permit key permitting transferring of said digital data, encrypting again said decrypted digital data to encrypted digital data by using said transfer permit key, and transferring said encrypted digital data.

2. A digital data management method according to claim **1**, wherein said utilization permit key includes a crypt key specific to said digital data.

3. A digital data management method according to claim **1**, wherein said utilization permit key includes a crypt key not specific to said digital data.

4. A digital data management method according to claim **1**, wherein:

said utilization permit key is hierarchized; and

said utilization permit key at an upper hierarchy level includes a function of said utilization permit key at a lower hierarchy level.

5. A digital management method according to claim **4**, wherein said transfer permit key is said utilization permit key at the highest hierarchy level.

6. A digital data management method according to claim **4**, wherein said edit permit key is said utilization permit key at the highest hierarchy level.

7. A digital data management method according to claim **1**, wherein:

said encrypted digital data is decrypted to decrypted digital data only when said digital data is displayed or edited; and

said decrypted digital data, when stored, copied or transferred, is encrypted again to said encrypted digital data.

8. A digital data management method according to claim **1**, wherein:

said encrypted digital data is, when displayed or edited, decrypted to said decrypted digital data; and

said decrypted digital data is, when stored, copied or transferred, encrypted again to said encrypted digital data.

9. A digital data management method according to claim **1**, further comprising a step of using a copyright management program for managing utilization of said digital data.

10. A digital data management method according to claim **9**, wherein said copyright management program is included in said utilization permit key.

11. A digital data management method according to claim **9**, wherein a crypt key is added to said copyright management program.

12. A digital data management method according to claim **9**, **10** or **11**, wherein said copyright management program is encrypted to an encrypted copyright management program.

13. A digital data management method according to claim **12**, wherein said encrypted copyright management program is decrypted by using said utilization permit key.

14. A digital data management method according to claim **9**, wherein said copyright management program is separate from said digital data.

15. A digital data management method according to claim **9**, wherein said copyright management program is integrated with said digital data.

16. A digital data management method according to claim **1**, wherein said utilization permit key includes a crypt key.

17. A digital data management method according to claim **9**, wherein said copyright management program includes said crypt key.

18. A digital data management method according to claim 16 or 17, wherein said crypt key is encrypted.

19. A digital data management method according to claim 1, wherein copyright information is added to said digital data.

20. A digital data control method according to claim 19, wherein said copyright information includes original copyright information and edit copyright information added to said digital data by a copyright management program.

21. A digital data management method according to claim 19, wherein said copyright information is added in a file body of said digital data.

22. A digital data management method according to claim 19, wherein said copyright information is added in a file header of said digital data.

23. A digital data management method according to claim 19, wherein said copyright information is added in a copyright management program.

24. A digital data management method according to claim 23, wherein said copyright management program is added in a file body of said digital data.

25. A digital data management method according to claim 19, wherein said copyright information must be present in order to use said digital data.

26. A digital data management method according to claim 25, wherein utilization of said digital data is managed by a copyright management program.

27. A digital data management method according to claim 25, wherein said digital data, excluding said copyright information, is encrypted again to said encrypted digital data by using said utilization permit key.

28. A digital data management method according to claim 25, wherein said digital data, excluding said copyright information, is encrypted again to said encrypted digital data by a copyright management program.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 7,036,019 B1
APPLICATION NO. : 09/544497
DATED : April 25, 2006
INVENTOR(S) : Makoto Saito

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 9

Lines 43-50, Claim 1 please delete "decrypting said encrypted digital data to decrypted digital data by using a display permit key, which is utilization permit key permitting displaying of said digital data, and displaying said decrypted digital data; decrypting said encrypted digital data to decrypted digital data by using a display permit key, which is said utilization permit key permitting displaying of said digital data, and displaying said decrypted digital data" and substitute --decrypting said encrypted digital data to decrypted digital data by using a display permit key, which is said utilization permit key permitting displaying of said digital data, and displaying said decrypted digital data--.

Signed and Sealed this

Thirteenth Day of April, 2010

David J. Kappos

David J. Kappos
Director of the United States Patent and Trademark Office